

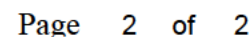


STATE OF COLORADO

Department of State

Page 1 of 2

ORDER		*****IMPORTANT*****				
Number:	PO,VAAA,202500006066	The order number and line number must appear on all invoices, packing slips, cartons, and correspondence.				
Date:	11/12/24	BILL TO				
Description:	VAAA, 2211 Legal Services Investigative	SECRETARY OF STATE 1700 BROADWAY #550 DENVER, CO 80290				
Effective Date:	11/12/24					
Expiration Date:	12/31/24					
BUYER		SHIP TO				
Buyer:	Georgia Roberts	SECRETARY OF STATE 1700 BROADWAY #550 DENVER, CO 80290				
Email:	georgia.roberts@coloradosos.gov					
VENDOR		SHIPPING INSTRUCTIONS				
Baird Quinn LLC 2036 East 17th Avenue Denver, CO 80206		Delivery/Install Date: FOB: FOB Dest, Freight Prepaid				
Contact:	Beth Doherty Quinn					
Phone:						
VENDOR INSTRUCTIONS						
EXTENDED DESCRIPTION						
Pursuant to Colorado Code of Regulations 101-1, Chapter 3-1.6.5 you are hereby notified that any and all provision(s) applied to this purchase that conflicts with Colorado law C.R.S. 24-106-109 are null and void. This purchase is subject to the State of Colorado Purchase Order Terms and Conditions which can be found at https://osc.colorado.gov/spco/ccu/purchase-order-terms-conditions. By accepting this purchase order and/or providing the goods and/or services to the State, you agree to be bound by and accept the State of Colorado Purchase Order Terms and Conditions unless there is a separate agreement with the State which governs. If this purchase contains any software or cloud computing products ("Software and Cloud Offerings"), each product will be subject to the State of Colorado Purchase Order Terms and Conditions which can be found at https://osc.colorado.gov/spco/ccu/purchase-order-terms-conditions. By accepting this purchase order and/or providing the software or cloud computing offerings to the State, you agree to be bound by and accept the State of Colorado Purchase Order Terms and Conditions unless there is a separate agreement with the State which governs.						
Line Item	Commodity/Item Code	UOM	QTY	Unit Cost	Total Cost	MSDS Req.



1	0	0.00	\$25,000.00	☐		
Description: Investigative Services						
Investigative Services hourly rates Beth Doherty Quinn \$390.00, John Quinn \$390.00, Paralegal \$150.00. Per the firms attached hourly agreement letter. The maximum amount for this PO is \$26,000.00 unless the PO and SOW are formally amended prior to services.						
Service From: 11/12/24		Service To: 12/31/24				
Line Item	Commodity/Item Code	UOM	QTY	Unit Cost	Total Cost	MSDS Req.
2			0	0.00	\$1,000.00	☐
Description: Investigative Services						
Investigative Services hourly rates Beth Doherty Quinn \$390.00, John Quinn \$390.00, Paralegal \$150.00. Per the firms attached hourly agreement letter. The maximum amount for this PO is \$25,000.00 unless the PO and SOW are formally amended prior to services.						
Service From: 11/12/24		Service To: 12/31/24				
TERMS AND CONDITIONS						
https://www.colorado.gov/osc/purchase-order-terms-conditions						
DOCUMENT TOTAL = \$26,000.00						

HOURLY FEE AGREEMENT

This document constitutes a binding and enforceable contract for professional services which supersedes any previous agreement. The parties to this contract are the Colorado Department of State, ("Client"), and Baird Quinn LLC, located at 2036 East Seventeenth Avenue, Denver, Colorado, 80206, ("Law Firm").

1. The Law Firm is hereby engaged by Client to conduct an external investigation. Law Firm's services are specifically limited to the matter described herein unless Client specifically requests, and Law Firm agrees in writing, to undertake additional work. This Hourly Fee Agreement specifically does not extend to litigation. Law Firm does not provide advice regarding any taxation issues and Client is specifically encouraged to obtain tax advice from a professional who specializes in such matters for any taxation issues that may arise, if any.

2. The Law Firm is hereby authorized to do all that is deemed necessary to provide services to the Client on the matter(s) described in Paragraph 1. The Law Firm strives to provide the highest quality service to Client and will use a reasonable degree of effort to represent the Client and provide the services in this matter. Law Firm relies on Client to disclose fully and accurately all facts and documents that may be materially relevant to the matter and to communicate regularly with Law Firm.

3. To the extent the subject matter of the representation involves claims brought against Client or claims that Client has against a third-party, which is unlikely to be applicable here, the Law Firm is not to settle or release any of the Client's claims or defenses without the consent of the Client. In such circumstances, the Client agrees to consider seriously any recommendation of settlement that the Law Firm makes.

4. The Law Firm will be entitled to receive attorneys' fees in the amount of **\$390.00 per hour** of attorney time for Beth Doherty Quinn, Esq., **\$390.00 per hour** for J. Mark Baird, Esq., and **\$145.00 per hour** of paralegal time. This time shall be billed in six (6) minute increments. The Client agrees to pay all attorneys' fees and costs incurred pursuant to this Hourly Fee Agreement.

5. It is anticipated that Beth Doherty Quinn, Esq., will be primarily responsible for performing the work hereunder, with paralegal assistance and/or assistance from Law Firm's other attorney(s). Law Firm shall determine which attorneys and/or staff shall perform the various aspects of the representation.

6. The Client has been informed and understands that there may be costs and expenses (aside from any attorney fee owed to the Law Firm under this Hourly Fee Agreement) incurred in representing the Client. All such costs are the Client's responsibility to pay. Examples of such expenses are fees of investigators, record collection charges, copy charges, service of process fees, messenger services, long distance telephone charges, parking expenses, express mail charges,

computerized research ("LEXIS"), or contract paralegal fees. The Law Firm agrees that future costs and expenses shall not exceed **\$1,000.00**.

7. The Client and Law Firm have agreed to waive the customary retainer fee, which is ordinarily charged by the Law Firm.

8. The Client and Law Firm have agreed that the fees charged under this Hourly Fee Agreement will not exceed **\$25,000.00**.

9. The Law Firm shall provide the Client with a periodic billing statement showing the costs and expenses incurred. The monthly billing statement shall be deemed accepted by the Client unless within fifteen (15) days of receipt of the billing statement, the Client advises the Law Firm in writing of any dispute that the Client has with the statement.

10. Except as otherwise provided between the parties, all monies due for attorneys' fees, costs and expenses shall be paid in full to the Law Firm within thirty (30) days of receipt of the billing statement. In the event that any invoice becomes past due, in whole or in part, for forty-five (45) days or more, the Client agrees that the Law Firm may withdraw from its representation of Client, or from its role as counsel of record, or both, as the case may be.

11. The Client agrees that the Law Firm shall have the right to withdraw from the Client representation in the event of: (a) the Client's non-cooperation; or (b) the Client's failure to comply with any provision of this Hourly Fee Agreement, including the failure to pay fees or costs due; and (c) for any other justifiable reason. The fact that the Law Firm justifiably withdraws its representation of the Client, or that the Client terminates its representation with the Law Firm, will not in any manner effect the Client's obligation to immediately pay the Law Firm for the costs or expenses owed, nor will such withdrawal or termination effect, release, or waive the Law Firm's entitlement to be compensated as set forth in this Hourly Fee Agreement.

12. In executing this Hourly Fee Agreement, the Client does not rely upon any inducements, promises, or representations other than what is explicitly set forth in this Hourly Fee Agreement. Specifically, the Law Firm does not guarantee any result for the Client.

13. By affixing the Client's signature below the Client affirms that the Client has read this entire document, that the Client has had ample opportunity to discuss its contents before signing it with the Law Firm, that the Client understands all terms and conditions, and that the Client is signing this Hourly Fee Agreement freely, voluntarily and without duress.

14. We are required by law to inform you of our policies regarding privacy of Client information. In the course of advising you, we may collect from you nonpublic personal information. You should know that all nonpublic personal information we receive from you is held in confidence and is not released to people outside the firm except as necessary to carry out our representation, as otherwise agreed to by you, or as required under applicable law. This does not limit the attorney-client privilege or the confidentiality rules to which Law Firm is subject,

both of which are governed by state law and by the rules of professional conduct. In order to guard your nonpublic personal information, we maintain physical, electronic and procedural safeguards that comply with these professional standards.

15. In the event of non-payment of fees, Law Firm may bring a proceeding against you to collect any unpaid fees and/or expenses. You shall be liable for all attorneys' fees and expenses incurred by Law Firm, including the value of attorneys' fees expended by attorneys within the Law Firm, in connection with any collection.

16. During Law Firm's representation of Client on a specific matter, Law Firm will likely obtain documents from the Client as well as from third parties related to the representation on that matter (the "Client File"). The Law Firm retains the Client File for seven (7) years after the completion of the Law Firm's work on the specific matter (the "Retention Period"). The Law Firm may retain the Client File in paper or electronic form. However the Law Firm will endeavor to return any original paper documents to client at the conclusion of the representation on the matter unless Client declines the return of such originals. At any time during the Retention Period, Client may request in writing that the Client File be returned to Client. If such a request is made, Law Firm will, within seven (7) business days of the written request, return the Client File by making it available at Law Firm's office. If Client would like to have the Client File delivered to Client, Client shall be responsible for the costs of such delivery.

17. This Hourly Fee Agreement constitutes the entire agreement between the Client and the Law Firm. Any changes, additions, or modifications must be in writing and signed by both the Client and the Law Firm.

DATED this ____ day of November, 2024.

By: _____, Client
Title: _____ for
Colorado Department of State

By: Baird Quinn LLC, Law Firm

Beth Doherty Quinn

by: Beth Doherty Quinn, Member/Partner

From: [Alonit Katzman](#)
To: [Carla Moore](#); [Samantha Ashton](#); [Georgia Roberts](#)
Cc: [Kathryn Mikeworth](#); [Brad Lang](#)
Subject: Enrollment in state vendor system and fee agreement: Baird Law Firm
Date: Friday, November 8, 2024 11:07:20 AM

Also, here is the confirmation that the vendor agreed to the terms of the purchase order.

Thanks,
Alonit

From: Beth Doherty Quinn [REDACTED]
Sent: Friday, November 8, 2024 10:45 AM
To: Alonit Katzman <Alonit.Katzman@ColoradoSOS.gov>
Subject: [EXTERNAL] RE: Request for availability for phone call

I have read and agree to the terms of the purchase order.

Beth Doherty Quinn
Baird Quinn LLC
2036 E. 17th Avenue
Denver, CO 80206
Main: [REDACTED]
Direct: [REDACTED]

CONFIDENTIALITY NOTICE: This e-mail message and any and all attachments may contain information that is confidential and/or subject to the attorney-client privilege or the attorney work product doctrine. This message, including attachments, if any, is intended solely for the use of the named recipient[s]. If you are not the intended recipient, you are hereby notified that any disclosure, copying or distribution of the contents of this transmission is prohibited. If you have received this message in error, please immediately delete and destroy the transmission and contact us at [REDACTED]

From: Alonit Katzman <Alonit.Katzman@ColoradoSOS.gov>
Sent: Friday, November 8, 2024 10:29 AM
To: Beth Doherty Quinn [REDACTED]
Subject: RE: Request for availability for phone call

Sorry, here is the purchase order.

Alonit

Baird Quinn LLC
The Bushong Mansion
2036 East 17th Avenue
Denver, CO 80206
EIN 27-3396559

Invoice submitted to:
Colorado Department of State
Georgia Roberts
via electronic mail:
georgia.roberts@coloradosos.gov
1700 Broadway, Suite 550
Denver, CO 80290

November 30, 2024
In Reference To: PO, VAAA,202500006066

VAAA,2211 Legal Services Investigative

Investigative Services hourly rates Beth Doherty Quinn \$390.00, John Baird \$390.00, Paralegal \$150.00. Per the firms attached hourly agreement letter. The maximum amount for this PO is \$26,000.00 unless the PO and SOW are formally amended prior to services.

Invoice #19691

Professional Services

		<u>Hrs/Rate</u>	<u>Amount</u>
11/13/2024	BDQ Review documents sent by client and create log (4.5); telephone call with K. Mikeworth and A. Katzman regarding questions about documents; setting up interview of [REDACTED], schedule for potential other interviews and logistics relating to interviews (.4)	4.90 390.00/hr	1,911.00
11/17/2024	BDQ Second review of key documents; drafting outline of questions for all witnesses	4.20 390.00/hr	1,638.00
11/18/2024	BDQ Contact E. Archenbault (attorney [REDACTED]) regarding scheduling a Zoom call	0.10 390.00/hr	39.00
	BDQ Zoom Interview of [REDACTED]	1.50 390.00/hr	585.00
11/19/2024	BDQ Review additional documents and information forwarded by A. Katzman including data sort of excel sheet to ID documents at issue (1.5); telephone call with A. Katzman re documents (.3); telephone call with C. Beall, A. Katzman, K. Mikeworth on status of investigation (.2); contact J. Morales (attorney [REDACTED]) regarding scheduling a meeting (.1).	2.10 390.00/hr	819.00

		Hrs/Rate	Amount
11/20/2024	BDQ Review notes for follow up questions ██████ (.5); continue Zoom teleconference interview of ██████ (1.5); email ██████ with file names for documents to be pulled (.2); finalize notes from ██████ (.4); review additional documents (1.00).	3.60 390.00/hr	1,404.00
	BDQ Prepare for interview with ██████; draft additional questions (.8); interview ██████ (1.0); communicate with A. Katzman regarding documents (.1) communicate with K. Milkworth re contact information (.1)	2.00 390.00/hr	780.00
11/21/2024	BDQ ID and print documents for review with ██████ in person interview (.7); consider and communicate to A. Katzman email/teams messages search terms (.4); review notes and prepare for interviews of ██████ and ██████ (.8); interview ██████ (1.0); interview ██████ (1.1); finalize notes interviews (.5)	4.50 390.00/hr	1,755.00
11/22/2024	BDQ Review relevant screenshots from ██████ (.1); email A. Katzman re same (.1); call and emails with A. Katzman re Varonis data search temporal parameters (.2); prepare Interviews with ██████ and ██████ (.5); attempt to contact ██████ at two phone numbers and an email (.1); contact potential forensic expert (.2); telephone call ██████ (.5); interview with ██████ (.6); telephone call with A. Katzman re email search, Varonis records scope, election rules, other matters (.2); follow up call with ██████ (.2); prepare for ██████ interview (1.0); interview ██████ in person (2.4); finalize notes from interviews of ██████, ██████ and ██████ (1.0).	7.10 390.00/hr	2,769.00
11/26/2024	BDQ Telephone call with K. Mikeworth	0.10 390.00/hr	39.00
11/27/2024	BDQ Review documents from ██████ re Last Pass notifications (.3); upload and attempt to review email documents (.2).	0.50 390.00/hr	195.00
11/29/2024	BDQ Review metadata again and compare hidden tabs within documents (.3); review and test A. Katzman spreadsheet (.6)	0.90 390.00/hr	351.00
11/30/2024	BDQ Review potentially relevant policies and begin drafting scope and policy section of report (3.5); identify questions for ██████ (.5); review new Varonis data (.2); review emails and teams messages (3.8); review transcript (.5)	8.50 390.00/hr	3,315.00
	For professional services rendered	40.00	\$15,600.00
	Additional Charges :		
11/30/2024	Court Costs / Fees		15.00
	Total costs		\$15.00
	Total amount of this bill		\$15,615.00

Amount

Balance due

\$15,615.00

Samantha Ashton

From: Chris Beall
Sent: Thursday, December 19, 2024 10:43 AM
To: Samantha Ashton; Brad Lang
Cc: Kathryn Mikeworth; Alonit Katzman
Subject: Payment approval for Baird Quinn invoice for investigative services
Attachments: (1) Deputy - Baird Quinn Invoice 19691_same as 12 Dec 2024.pdf

Follow Up Flag: Follow up
Flag Status: Flagged

Brad/Sam,

I have reviewed the invoice from Baird Quinn LLC for its work on the outside investigation of the office's password exposure matter, and this is approved for payment.

Thanks,
Chris



Christopher P. Beall
Deputy Secretary of State
303.549.0000
Chris.Beall@ColoradoSoS.gov
1700 Broadway, Suite 550
Denver, CO 80290

Acceptable Use Policy (AUP)

Colorado Department of State Acceptable Use of State Data and IT Resources

Contents

1.	Purpose	2
2.	Scope and Application.....	2
3.	Acceptable Use	3
4.	Prohibited Activities.....	3
5.	Data Protection and System Security	4
6.	Communication Standards.....	6
7.	Device and Software Management	6
8.	Data Protection Requirements.....	7
9.	Remote Access, Authentication, and Devices.....	7
10.	Personal Use of State IT Resources.....	8
11.	Use of Personally Owned Equipment	8
12.	Training	9
13.	Compliance.....	9
14.	Monitoring and Enforcement	10
15.	Annual Acceptance, Retention, and Expiration.....	10
16.	Definitions	11
17.	Revision History	12
18.	Acknowledgment.....	13

1. Purpose

- A. The Colorado Department of State (CDOS) relies on secure and efficient information technology systems to fulfill its mission. This Acceptable Use Policy (AUP) establishes guidelines for the responsible use of State of Colorado (State) and CDOS technology resources, protecting the confidentiality, integrity, and availability of information assets.
- B. The policy provides clear standards for CDOS:
 - 1. Safe and appropriate use of computing systems
 - 2. Management of equipment and software requests
 - 3. Licensing compliance
 - 4. IT support services
 - 5. Protection of information and resources
- C. This Policy is intended to meet the State of Colorado's Cyber Security Policies. The Colorado Cyber Security Policies can be found on the State of Colorado's website at <https://oit.colorado.gov/standards-policies-guides/technical-standards-policies#information>. This policy supports the State of Colorado in achieving requirements of the Colorado Information Security Act (C.R.S. 24-37.5-401 et seq.)

2. Scope and Application

- A. Who Must Comply
This policy governs all individuals accessing CDOS and State technology resources on behalf of the Department, including:
 - 1. Employees
 - 2. Contractors
 - 3. Connected partners
 - 4. Visitors
 - 5. Volunteers
- B. Resources Covered
State and CDOS:
 - 1. Owned and managed technology
 - 2. Intellectual property
 - 3. Data, systems, and networks
 - 4. Computing devices
- C. All State IT resources, information, and data are the sole property of the State of Colorado, and applicable statutes, policies and guidelines govern their use. All users must use State and CDOS IT resources in accordance with this policy.
- D. This policy is not intended to govern the use of State IT resources made available for public use (e.g., public Wi-Fi in State facilities by members of the public).

3. Acceptable Use

- A. Computer resources and data are to be used for Departmental business only. These resources are vital to the function and continuance of the organization. Access to these resources is granted to staff, partners, and designees for the purpose of accomplishing their job functions or contractual obligations.
- B. CDOS users are required to adhere to all applicable Federal, Colorado, and local laws. In addition to this policy, users are also required to adhere to the State of Colorado's Cyber Security Policies as well as the Department of State Employee Handbook, and other Department of State policies.

4. Prohibited Activities

- A. Department of State IT Resources, Networks, Systems, Email, and Internet access may not be used to:
 - 1. Communicate unethical, racial, sexual, obscene, harassing, or improper material.
 - 2. Send or willfully receive any unethical, harassing, threatening, obscene, racist, sexist, or sexual documents, pictures, videos, software, or data.
 - 3. Send outside the Department any sensitive, proprietary, confidential, or Personally Identifiable Information (PII) without a Director's or their designee's authorization.
 - 4. Send or download any software, including but not limited to shareware, freeware, or browser controls/plugins without proper Information Technology approval.
 - 5. Send or download copyright-protected material owned by a private, commercial third-party unless authorized by the copyright holder or by Director or their designee's authorization.
 - 6. Create false or misleading information (either individually or by masquerading).
 - 7. Violate Federal, Colorado, or local laws or regulations.
 - 8. Violate Department policies or procedures.
 - 9. Violate any of the State of Colorado Universal Policies, or any of the Colorado Information Security Policies.
 - 10. Disrupt CDOS or other site's operations.
 - 11. Abuse the rights of others.
 - 12. Engage in unauthorized activities in support of or opposition to candidates or campaign issues.
 - 13. Play Internet Games, except for authorized team building exercises on approved sites.
 - 14. Use chargeable Internet Service Provider(s) services or fee-for-services or downloads from other sites for personal use.
 - 15. Access proxies or other services to bypass the Department's security controls unless given written permission by CDOS Information Technology Senior Management to meet a specific business need.
 - 16. Intentionally bypass system or network security controls unless given permission from IT management for the purpose of troubleshooting systems or completing a specific system task with compensating controls in place.
 - 17. Use State or IT resources for any commercial purpose or personal financial gain.
 - 18. Forward State email to a personal email account if it contains State data or information unless explicitly approved by user's appointing authority. An exception is provided for email related to the employee, such as State benefits, paystubs, tax forms, PERA or personal growth (e.g., certificates of course completions).

19. Use State IT resources in a manner that jeopardizes the confidentiality, integrity, or availability of the IT resources.
20. Gain or attempt to gain unauthorized access to systems or data the user does not have authorization to access.
21. Administrators may not open or review files they are not authorized to review or access even if they have permissions to administer files by maintaining backups, access controls, and other general administrative functions.

5. Data Protection and System Security

A. Domain user IDs, System Accounts, and Passwords

1. Each user will be given a unique user ID for access to Department of State technology resources.
2. Passwords must be chosen carefully and kept private.
3. After 4 incorrect login attempts, the account will be locked out.
4. Passwords will expire every [REDACTED] days.
5. Users must log out or lock their screen when away from their computer.
6. Users are not allowed to share their passwords or try to obtain passwords for other accounts.
7. All passwords must meet complexity requirements as noted in sub-section 5.C.
8. Supervisors and staff must notify IT of any staff members that are going to be out of the office and not working for longer than three weeks. Accounts must be disabled if they are not used for a period of three weeks or more.

B. Other Credential, Password, and Sensitive Authentication Management

1. Users must use the Department-provided password safe for storing and sharing passwords.
2. Privileged credentials, authentication credentials, access control credentials, encryption keys, authentication certificates, and access tokens must be stored in the Department-provided password safe.
3. Storage of passwords in databases must be protected with encryption and complex passwords.
4. Any exception to this policy must be approved by a Division Director or Deputy Director responsible for data and the IT Division Director or Deputy IT Division Director.

C. Password Requirements and Multi-factor Authentication (MFA)

1. All passwords are required to be [REDACTED] characters long at a minimum and must consist of a combination of at least three out of four of the following: uppercase letters, lower case letters, numbers, and symbols.
2. Good passwords are long and are not easy to guess. Passphrases may be used and are encouraged as long as those passphrases are not common phrases or sayings.
3. [REDACTED]
4. Users should not write down their passwords or have any keys or hints somewhere exposed that could lead to an account compromise.

5. Users should not use a 'password scheme' where the password is the same and simply changes a single word number or symbol. This practice puts the Department and State systems at risk.

D. Users should not use passwords that could possibly be guessed or constructed by an attacker reviewing information on social media or other sites.

1. Users should not use the same passwords on different systems or use the same password at work as they do at home or on other sites.
2. Multi-factor authentication should be used on any systems that have an MFA option available. Exceptions to this may be granted whenever a system can only be accessed from another system that already requires multi-factor authentication.
 - Example: Logging into your laptop requires MFA via a token authenticator. If after you log in to your workstation and there is another resource that can only be accessed once authenticated with your laptop, it may be permitted to not require your MFA token code again, to access that resource, such as another workstation or jump box. (MFA – See Definitions Section)
3. IT Help Desk Staff, Administrators, and other users who issue passwords should meet these same requirements when generating a new password for a user initially logging in to a new system and/or for a user that has forgotten their password.

E. File Safety

1. Users are permitted to only store mission-critical data on assigned cloud storage or network drives.
2. Storing any data, even non-critical data, on removable media or local hard drives is not recommended and not backed up.

F. Information containing credit card numbers, confidential information, or Personally Identifiable Information (PII) may not be emailed, transmitted, or stored on removable media without proper encryption.

G. Data Protection and Handling

1. Users are prohibited from sending, requesting, or disseminating Personally Identifiable Information (PII) or other sensitive information in an unencrypted form over a State network, email, or the internet. Any sensitive data that needs to be transmitted or sent (data in transit), must be encrypted with supplied platforms for email encryption or other file encryption methods such as encrypted compressed (zip) files or encrypted document storage.
2. Users must protect State data from unauthorized use, access or disclosure, and State data must never be downloaded to or stored on personal devices.
3. All mobile devices (i.e., laptops, mobile phones) used for State business must have encryption at rest enabled. (Encryption at rest – See Definitions section)

H. Artificial intelligence (AI)

1. All use of AI must be approved by IT and Division Management before use.
2. All users must be trained on proper AI use before use and abide by all State and Department AI policies.

6. Communication Standards

A. Internet, Email, and Systems Use

1. CDOS networks are for business use, with limited personal use permitted.
2. Only Department and State of Colorado configured Internet connections may be used.
3. Department-issued equipment connecting to third-party networks must use the CDOS VPN.
4. All e-mail sent to and from Department-assigned e-mail accounts is property of CDOS.
5. Caution should be used when accessing email attachments or links.
6. Use of CDOS email addresses in non-business-related forums is prohibited.
7. The rule of "least privilege" (only necessary Internet services will be granted to perform a particular job function) will be used in granting access to Internet services. Further, Internet addresses of sites which contain racist, sexist, sexual, obscene, harassing, criminal, or other information which violate local, State, Federal laws, or regulations, or CDOS policies and procedures may be blocked.

B. Office Representation on the Internet (Social Media)

1. Employees should exercise discretion when posting on personal social networking sites to ensure that they do not reflect poorly on the Department or the Secretary of State.
2. Please refer to the Employee Handbook for more information on the Social Media policy.

7. Device and Software Management

A. Hardware/Software Requests

1. All software and hardware installed on or connected to Department devices must have written approval from the Information Technology Division or be provided by the Information Technology Division.
2. Removable media and hardware not issued by the Department is not permitted to connect to Department computer systems without documented approval.
3. Approved software lists will be maintained by the IT Division for reference.
4. All new hardware and software requests, beyond previously-approved equipment and software, must first be approved by the requesting user's Division Director or Deputy Director before being reviewed by IT.
5. Software and hardware must be reviewed for fundamental cybersecurity standards before connecting to the CDOS network.
6. No employee or contractor may knowingly violate third-party intellectual property rights or software license agreements.

B. Remote Access and Control

1. Users are responsible for their network use and must never relinquish control of their systems to non-Department technical support without approval. In addition, users should continue to monitor all activity even when and if approved.
2. Remote Access and Remote-Control software is only permitted after approval from Information Technology.

C. Change Management

1. All users with rights and the authority to administer systems, alter system functionality, install software, change configurations, publish code, or otherwise change a network or system device beyond standard use must have the proper authority within their job function and use change management for proper approvals, communication, and documentation of system changes.

8. Data Protection Requirements

A. Data Ownership

1. Ownership of data will reside with the Department or Division Director responsible for the data. Access permissions must be granted by the data owner or their designee before a user may attempt access.

B. File Shares and Drives

1. Each Division will have shared information drives and SharePoint sites.
2. Access to Division's drives and sites are set by the CDOS management and the Division's Director.
3. System Administrators will not view file contents without permission, except as necessary for their job functions.

C. Home Directories and Cloud Storage Drives

1. Each user will have Cloud Storage Drives and a Home Directory (H: Drive).
2. Users are encouraged to primarily use Cloud Storage Drives.
3. System Administrators may not view file contents without permission, except as necessary for their job functions.

D. Protecting Devices and State Data

1. All Users must take reasonable precautions to avoid the loss or theft of IT resources used for State business.
2. Devices used for State business, including personal devices, that are lost or stolen must be reported immediately to the user's manager and the IT Help Desk. The IT Help Desk will forward reports to the cybersecurity team.
3. It is not permissible for a user to save work-related products of any type (e.g., documents, spreadsheets, etc.) to personal devices or personal removable media (e.g., flash drives, etc.).

E. Suspicious Activity Reporting

1. Users are required to report suspicious activities or incidents to the IT Help Desk, which will then report to the Information Security group.
2. Suspicious and potential phishing emails should be reported with tools provided in the email system and Department ticketing systems.

9. Remote Access, Authentication, and Devices

A. Remote Access

1. Connecting to internal State network resources must be done through approved remote access processes, using VPN for State computing resources accessible only on the trusted State private network; direct access is prohibited.
2. Users may not remotely access a CDOS or State IT resource via a personal device unless approved by the appointing authority.

B. International Access to State Data and IT Resources

1. International user access to systems and data from high-risk countries as defined by the State Department's International Traffic in Arms Regulations (ITAR) list is prohibited.
2. International user access to systems and data may be prohibited by laws governing specific data types, including but not limited to CJIS and FTI.
3. Users should reference CDOS HR policies and abide by State Policies for working out of State of Colorado and/or the country.
4. Accessing State or CDOS resources from other countries for any period of time must be approved by Human Resources and Information Technology.

10. Personal Use of State IT Resources

- A. Only minimal, incidental personal use of State resources such as email is allowed and never for political, business or any purpose that conflicts with State ethics requirements or State policies, and/or the Department's conflict of interest policy. (Reference Governor's Office of Information Technology Acceptable Use Policy (AUP) Adopted 12/19/2024 - <https://oit.colorado.gov/standards-policies-guides/technical-standards-policies>)

11. Use of Personally Owned Equipment

- A. When a user has been approved to use their personal device as their primary work device, they are responsible for ensuring that any device used to connect to a State IT resource is secured consistent with best practices for the use of personal computing devices, including without limitation:
1. Ensure the device is free from malware infections.
 2. The device is protected by strong authentication.
 3. The device operating system and software are updated and current according to State standards.
 4. The device is utilizing full disk encryption.
 5. The device is not storing State data.
- B. Users are prohibited from using personally owned devices to access, store, or process State data without written authorization from both their Division Director or Deputy and the Director of Information Technology, Deputy Director of Information Technology, or the Appointing Authority.
- C. CDOS staff are permitted to use personal mobile devices for MFA authentication applications such as RSA Authentication, Google Authenticator, Last Pass Authenticator, and other authenticators listed on the Approved software list.
- D. It is not permissible to save work-related products of any type (e.g., documents, spreadsheets, etc.) to user personal devices or personal removable media (e.g., flash drives, etc.).

12. Training

A. Cybersecurity Training

1. All users are required to complete mandatory cybersecurity training at least annually and throughout the year as assigned.
2. Users may be assigned additional cybersecurity or other training as necessary to ensure proper system use and security.

B. Software and Systems Training

1. Users in different divisions (Business, Elections, Administration, Information Technology) have distinct roles and responsibilities. Managers, in coordination with users, must determine training needs to ensure the proper handling of data and the proper use of Information Technology.
2. Users are required, according to their job function, to research and learn about the technologies needed to effectively complete their work. Users should work with their supervisor to determine their training needs.

13. Compliance

A. Privacy

1. Information transmitted through unsecured systems should not be considered private.
2. All transmissions are business records and subject to inspection, review, or disclosure as required by law.
3. The Department reserves the right to access and disclose all information sent, received, or stored through its systems.

B. License Agreements/Copyright Compliance

1. State IT resources must be used in accordance with the terms of software license agreements or other copyright restrictions to protect the state, its officials, and Users from possible legal action. Users may not access or store any copyrighted material using any State IT resource without an appropriate license.
2. The Department may be financially liable for unauthorized use of copyright-protected or licensed material and may seek restitution from employees responsible for unauthorized use of copyright-protected or licensed material.

C. Criminal Activity

1. Information created, collected, generated, or stored by a user on either State-owned computing devices or personal computing devices that are authorized to connect to State IT resources may be disclosed to State risk management, State human resources, Department human resources and State law enforcement if criminal activity is suspected. This disclosure will be at the discretion of CDOS Information Technology Senior Management, the User's appointing authority and State human resources, as applicable, during or after the course of investigating suspected acceptable use violations.

D. Employment Termination

1. As soon as possible prior to, and in all events at the latest upon the date of, termination of employment, Information Technology must be notified immediately to remove access to a user's various systems and facilities.

14. Monitoring and Enforcement

A. Information Systems and Security Operations

1. Information Technology management and the cybersecurity team will collaborate to monitor systems, collect logs, and conduct security assessments to verify compliance with established safeguards and behaviors outlined in this policy. Security personnel and system administrators will perform regular audits of system access, review application logs, monitor network traffic, conduct penetration testing, and execute other security-related functions as authorized by CDOS Information Technology Senior Management or the State Chief Information Security Officer.
2. Systems administrators will back up, delete, retain, and restore data in alignment with the Department data retention policies.

B. Surveillance Authority

1. CDOS IT management, supervisors, and security personnel maintain the right to monitor all computing activities without prior notification. This monitoring encompasses all system access, including but not limited to Internet usage, file access, and email communications.
2. Any public agency has the right to monitor and/or investigate their users' activity while accessing State network, internet, system or email accounts and their usage, whether on a State-issued or personal device authorized to connect to the State network. (CISP-018)

C. Privacy and Colorado Open Records Act (CORA)

1. Users have no expectation of privacy while using State resources or technology. All electronic communications sent to and from State-assigned accounts are the property of the State of Colorado.
2. Electronic communications pertaining to State business are subject to the Colorado Open Records Act (CORA, C.R.S. § 24-72-201 et seq.). Any communication using personal equipment, such as personal phones or laptops, is also subject to CORA to the extent it pertains to State business.

15. Annual Acceptance, Retention, and Expiration

- A. This policy must be accepted by Users at the start of employment and no less frequently than annually thereafter.
- B. The following must be done by Agency and Users:
 1. CDOS provides a documented acknowledgment of these rules for Users to read and sign before accessing the system.
 2. CDOS maintains a record of signed acknowledgments for appropriate retention periods.
 3. CDOS requires individuals to re-read and re-sign the rules annually, regardless of prior acknowledgments.
- C. This policy remains in effect until superseded or rescinded by the CDOS Chief Information Security Officer or CDOS Chief Information Officer.

16. Definitions

- A. Access: The time when an individual is permitted into a security point or system. Access also means the authority to access restricted facts, information, or records.
- B. Appointing Authority: As defined in Board Rule 1-8, refers to the executive director of principal departments or their delegate(s).
- C. CDOS Information Technology Senior Management – Chief Information Officer, Deputy Chief Information Officer, Chief Information Security Officer, and Chief Technology Officer.
- D. CJIS Data: Refers to Criminal Justice Information Services, including fingerprints, criminal background checks, etc. CJIS includes Criminal history record information from the FBI; however, PII obtained through public records/court documents typically is no longer protected (once published).
- E. Credentials and secrets: In computer networks, secrets are sensitive digital credentials that provide access to systems, services, and data. Think of them as special keys that allow different parts of our technology systems to communicate securely with each other. Unlike regular passwords that humans use, secrets are designed to be used by machines, applications, and automated processes. Examples include:
 - 1. API keys that allow applications to communicate with each other,
 - 2. digital certificates for secure website connections,
 - 3. database passwords for accessing stored information,
 - 4. SSH keys for secure remote system access,
 - 5. encryption keys that scramble sensitive data,
 - 6. security tokens for temporary system access,
 - 7. private certificates for secure data transmission,
 - 8. cloud service credentials.
- F. Data Owner: CDOS Division Directors are ultimately responsible for the data that their Division is responsible for or maintains. Directors may designate staff as owners of specific datasets. Data owners and their designees are responsible for maintaining, reviewing, and ensuring proper data handling as outlined in this policy.
- G. Disclosure of Information: Making facts or information known to an individual, group or the public.
- H. Encryption at rest: Hard disk or local storage encryption, in other words, data that is stored or “at rest” and not “in transit”.
- I. IT Resource: Any computing device or resource, including but not limited to desktop computers, laptops, tablets (e.g., iPad, Windows, Chromebook, etc.); smartphones (e.g., iPhone, Android, etc.), removable media that has the ability to access IT resources, including IT networks; and accounts that allow access to IT resources (e.g., email, cloud-based software and applications, etc.).
- J. Multi-factor authentication: Consists of something you know like a password, something you have like a security token or authentication device, or something you are, such as your fingerprint. Two-factor MFA is reached when you use two of the three above to authenticate with a system.
- K. PII: Any information that can be used by itself or combined with other personal or identifying information to uniquely identify, contact or locate a specific person.

- L. Remote Access: Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network. (e.g., the Internet)
- M. Removable Media: Any type of storage device that can be removed from an IT resource to which it has been connected or attached, including but not limited to any USB drive (also called flash drive or thumb drive), hard drive, personal music player, disc drive, DVD, CD, camera, mobile phone, memory card, etc.
- N. Sensitive Data or Information: Information whose loss, misuse, or unauthorized access to or modification of which could adversely affect the interests or the ability of the Department or State to conduct day-to-day operations or the privacy of individual persons. Sensitive data or information includes, but is not limited to FTI, PII, PHI, CJI, etc. See TS-CISO-001 Data Security (posted on OIT’s website at Technical Standards & Policies).
- O. Unauthorized Access: A person gains logical or physical access without permission to a network, system, application, data, information, records, or other resource.

17. Revision History

<i>Review Date</i>	<i>Reviewed By</i>	<i>Revisions</i>
01/20/2025	Rich Schliep	Initial Draft
01/20/2026	Gregory Williams	Version 1

18. Acknowledgment

All users of CDOS networks as defined in the scope (Section 2) must sign this Acceptable Use Policy (AUP), agreeing to adhere to all policies and guidelines contained therein.

Any violation of the behaviors and safeguards established in this document constitutes unacceptable use and shall result in disciplinary measures. Such measures may include:

- Mandatory security awareness training
- Immediate access revocation
- Financial liability for damages
- Employment suspension or termination
- Civil or criminal prosecution under applicable laws

A violation of this policy by temporary workers, interns, volunteers, contractors, or vendors may result in termination of their contract or assignment with the State of Colorado or Colorado Department of State.

The Department reserves the right to implement any combination of these measures based on the severity and nature of the violation.

I acknowledge that I have read and understand the Acceptable Use Policy for State Data and IT Resources.

I agree to strictly abide by these policies and procedures and acknowledge that when an instance of non-compliance is suspected or discovered, proper disciplinary action may be taken, up to and including termination in accordance with Colorado regulations. Criminal or civil action may be initiated where appropriate.

Jena Griswold

Employee Name (printed)

Signed by:

Jena Griswold

1971F3C99C634D5...

Employee Signature

Administration

Division (printed)

February 6, 2026

Date

Signed by:

Chad Cornelius

C443FC763041492...

Chief Information Officer Signature

February 7, 2026

Date

Acceptable Use Policy (AUP)

Colorado Department of State Acceptable Use of State Data and IT Resources

Contents

- 1. Purpose.....2
- 2. Scope and Application.....2
- 3. Acceptable Use.....3
- 4. Prohibited Activities.....3
- 5. Data Protection and System Security4
- 6. Communication Standards5
- 7. Device and Software Management6
- 8. Data Protection Requirements6
- 9. Remote Access, Authentication, and Devices7
- 10. Personal Use of State IT Resources.....8
- 11. Use of Personally Owned Equipment8
- 12. Training.....8
- 13. Compliance9
- 14. Monitoring and Enforcement.....9
- 15. Annual Acceptance, Retention, and Expiration 10
- 16. Definitions 10
- 17. Revision History 12
- 18. Acknowledgment 13

1. Purpose

- A. The Colorado Department of State (CDOS) relies on secure and efficient information technology systems to fulfill its mission. This Acceptable Use Policy (AUP) establishes guidelines for the responsible use of State of Colorado (State) and CDOS technology resources, protecting the confidentiality, integrity, and availability of information assets.
- B. The policy provides clear standards for CDOS:
 - 1. Safe and appropriate use of computing systems
 - 2. Management of equipment and software requests
 - 3. Licensing compliance
 - 4. IT support services
 - 5. Protection of information and resources
- C. This Policy is intended to meet the State of Colorado's Cyber Security Policies. The Colorado Cyber Security Policies can be found on the State of Colorado's website at <https://oit.colorado.gov/standards-policies-guides/technical-standards-policies#information>. This policy supports the State of Colorado in achieving requirements of the Colorado Information Security Act (C.R.S. 24-37.5-401 et seq.)

2. Scope and Application

- A. Who Must Comply
This policy governs all individuals accessing CDOS and State technology resources on behalf of the Department, including:
 - 1. Employees
 - 2. Contractors
 - 3. Connected partners
 - 4. Visitors
 - 5. Volunteers
- B. Resources Covered
State and CDOS:
 - 1. Owned and managed technology
 - 2. Intellectual property
 - 3. Data, systems, and networks
 - 4. Computing devices
- C. All State IT resources, information, and data are the sole property of the State of Colorado, and applicable statutes, policies and guidelines govern their use. All users must use State and CDOS IT resources in accordance with this policy.
- D. This policy is not intended to govern the use of State IT resources made available for public use (e.g., public Wi-Fi in State facilities by members of the public).

3. Acceptable Use

- A. Computer resources and data are to be used for Departmental business only. These resources are vital to the function and continuance of the organization. Access to these resources is granted to staff, partners, and designees for the purpose of accomplishing their job functions or contractual obligations.
- B. CDOS users are required to adhere to all applicable Federal, Colorado, and local laws. In addition to this policy, users are also required to adhere to the State of Colorado's Cyber Security Policies as well as the Department of State Employee Handbook, and other Department of State policies.

4. Prohibited Activities

- A. Department of State IT Resources, Networks, Systems, Email, and Internet access may not be used to:
 - 1. Communicate unethical, racial, sexual, obscene, harassing, or improper material.
 - 2. Send or willfully receive any unethical, harassing, threatening, obscene, racist, sexist, or sexual documents, pictures, videos, software, or data.
 - 3. Send outside the Department any sensitive, proprietary, confidential, or Personally Identifiable Information (PII) without a Director's or their designee's authorization.
 - 4. Send or download any software, including but not limited to shareware, freeware, or browser controls/plugins without proper Information Technology approval.
 - 5. Send or download copyright-protected material owned by a private, commercial third-party unless authorized by the copyright holder or by Director or their designee's authorization.
 - 6. Create false or misleading information (either individually or by masquerading).
 - 7. Violate Federal, Colorado, or local laws or regulations.
 - 8. Violate Department policies or procedures.
 - 9. Violate any of the State of Colorado Universal Policies, or any of the Colorado Information Security Policies.
 - 10. Disrupt CDOS or other site's operations.
 - 11. Abuse the rights of others.
 - 12. Engage in unauthorized activities in support of or opposition to candidates or campaign issues.
 - 13. Play Internet Games, except for authorized team building exercises on approved sites.
 - 14. Use chargeable Internet Service Provider(s) services or fee-for-services or downloads from other sites for personal use.
 - 15. Access proxies or other services to bypass the Department's security controls unless given written permission by CDOS Information Technology Senior Management to meet a specific business need.
 - 16. Intentionally bypass system or network security controls unless given permission from IT management for the purpose of troubleshooting systems or completing a specific system task with compensating controls in place.
 - 17. Use State or IT resources for any commercial purpose or personal financial gain.
 - 18. Forward State email to a personal email account if it contains State data or information unless explicitly approved by user's appointing authority. An exception is provided for email related to the employee, such as State benefits, paystubs, tax forms, PERA or personal growth (e.g., certificates of course completions).
 - 19. Use State IT resources in a manner that jeopardizes the confidentiality, integrity, or availability of the IT resources.

20. Gain or attempt to gain unauthorized access to systems or data the user does not have authorization to access.
21. Administrators may not open or review files they are not authorized to review or access even if they have permissions to administer files by maintaining backups, access controls, and other general administrative functions.

5. Data Protection and System Security

A. Domain user IDs, System Accounts, and Passwords

1. Each user will be given a unique user ID for access to Department of State technology resources.
2. Passwords must be chosen carefully and kept private.
3. After 4 incorrect login attempts, the account will be locked out.
4. Passwords will expire every [REDACTED] days.
5. Users must log out or lock their screen when away from their computer.
6. Users are not allowed to share their passwords or try to obtain passwords for other accounts.
7. All passwords must meet complexity requirements as noted in sub-section 5.C.
8. Supervisors and staff must notify IT of any staff members that are going to be out of the office and not working for longer than three weeks. Accounts must be disabled if they are not used for a period of three weeks or more.

B. Other Credential, Password, and Sensitive Authentication Management

1. Users must use the Department-provided password safe for storing and sharing passwords.
2. Privileged credentials, authentication credentials, access control credentials, encryption keys, authentication certificates, and access tokens must be stored in the Department-provided password safe.
3. Storage of passwords in databases must be protected with encryption and complex passwords.
4. Any exception to this policy must be approved by a Division Director or Deputy Director responsible for data and the IT Division Director or Deputy IT Division Director.

C. Password Requirements and Multi-factor Authentication (MFA)

1. All passwords are required to be [REDACTED] characters long at a minimum and must consist of a combination of at least three out of four of the following: uppercase letters, lower case letters, numbers, and symbols.
2. Good passwords are long and are not easy to guess. Passphrases may be used and are encouraged as long as those passphrases are not common phrases or sayings.
3. [REDACTED]
4. Users should not write down their passwords or have any keys or hints somewhere exposed that could lead to an account compromise.
5. Users should not use a 'password scheme' where the password is the same and simply changes a single word number or symbol. This practice puts the Department and State systems at risk.

- D. Users should not use passwords that could possibly be guessed or constructed by an attacker reviewing information on social media or other sites.
 - 1. Users should not use the same passwords on different systems or use the same password at work as they do at home or on other sites.
 - 2. Multi-factor authentication should be used on any systems that have an MFA option available. Exceptions to this may be granted whenever a system can only be accessed from another system that already requires multi-factor authentication.
 - Example: Logging into your laptop requires MFA via a token authenticator. If after you log in to your workstation and there is another resource that can only be accessed once authenticated with your laptop, it may be permitted to not require your MFA token code again, to access that resource, such as another workstation or jump box. (MFA – See Definitions Section)
 - 3. IT Help Desk Staff, Administrators, and other users who issue passwords should meet these same requirements when generating a new password for a user initially logging in to a new system and/or for a user that has forgotten their password.
- E. File Safety
 - 1. Users are permitted to only store mission-critical data on assigned cloud storage or network drives.
 - 2. Storing any data, even non-critical data, on removable media or local hard drives is not recommended and not backed up.
- F. Information containing credit card numbers, confidential information, or Personally Identifiable Information (PII) may not be emailed, transmitted, or stored on removable media without proper encryption.
- G. Data Protection and Handling
 - 1. Users are prohibited from sending, requesting, or disseminating Personally Identifiable Information (PII) or other sensitive information in an unencrypted form over a State network, email, or the internet. Any sensitive data that needs to be transmitted or sent (data in transit), must be encrypted with supplied platforms for email encryption or other file encryption methods such as encrypted compressed (zip) files or encrypted document storage.
 - 2. Users must protect State data from unauthorized use, access or disclosure, and State data must never be downloaded to or stored on personal devices.
 - 3. All mobile devices (i.e., laptops, mobile phones) used for State business must have encryption at rest enabled. (Encryption at rest – See Definitions section)
- H. Artificial intelligence (AI)
 - 1. All use of AI must be approved by IT and Division Management before use.
 - 2. All users must be trained on proper AI use before use and abide by all State and Department AI policies.

6. Communication Standards

- A. Internet, Email, and Systems Use
 - 1. CDOS networks are for business use, with limited personal use permitted.
 - 2. Only Department and State of Colorado configured Internet connections may be used.
 - 3. Department-issued equipment connecting to third-party networks must use the CDOS VPN.
 - 4. All e-mail sent to and from Department-assigned e-mail accounts is property of CDOS.

5. Caution should be used when accessing email attachments or links.
6. Use of CDOS email addresses in non-business-related forums is prohibited.
7. The rule of "least privilege" (only necessary Internet services will be granted to perform a particular job function) will be used in granting access to Internet services. Further, Internet addresses of sites which contain racist, sexist, sexual, obscene, harassing, criminal, or other information which violate local, State, Federal laws, or regulations, or CDOS policies and procedures may be blocked.

B. Office Representation on the Internet (Social Media)

1. Employees should exercise discretion when posting on personal social networking sites to ensure that they do not reflect poorly on the Department or the Secretary of State.
2. Please refer to the Employee Handbook for more information on the Social Media policy.

7. Device and Software Management

A. Hardware/Software Requests

1. All software and hardware installed on or connected to Department devices must have written approval from the Information Technology Division or be provided by the Information Technology Division.
2. Removable media and hardware not issued by the Department is not permitted to connect to Department computer systems without documented approval.
3. Approved software lists will be maintained by the IT Division for reference.
4. All new hardware and software requests, beyond previously-approved equipment and software, must first be approved by the requesting user's Division Director or Deputy Director before being reviewed by IT.
5. Software and hardware must be reviewed for fundamental cybersecurity standards before connecting to the CDOS network.
6. No employee or contractor may knowingly violate third-party intellectual property rights or software license agreements.

B. Remote Access and Control

1. Users are responsible for their network use and must never relinquish control of their systems to non-Department technical support without approval. In addition, users should continue to monitor all activity even when and if approved.
2. Remote Access and Remote-Control software is only permitted after approval from Information Technology.

C. Change Management

1. All users with rights and the authority to administer systems, alter system functionality, install software, change configurations, publish code, or otherwise change a network or system device beyond standard use must have the proper authority within their job function and use change management for proper approvals, communication, and documentation of system changes.

8. Data Protection Requirements

A. Data Ownership

1. Ownership of data will reside with the Department or Division Director responsible for the data. Access permissions must be granted by the data owner or their designee before a user may attempt access.

B. File Shares and Drives

1. Each Division will have shared information drives and SharePoint sites.
2. Access to Division's drives and sites are set by the CDOS management and the Division's Director.
3. System Administrators will not view file contents without permission, except as necessary for their job functions.

C. Home Directories and Cloud Storage Drives

1. Each user will have Cloud Storage Drives and a Home Directory (H: Drive).
2. Users are encouraged to primarily use Cloud Storage Drives.
3. System Administrators may not view file contents without permission, except as necessary for their job functions.

D. Protecting Devices and State Data

1. All Users must take reasonable precautions to avoid the loss or theft of IT resources used for State business.
2. Devices used for State business, including personal devices, that are lost or stolen must be reported immediately to the user's manager and the IT Help Desk. The IT Help Desk will forward reports to the cybersecurity team.
3. It is not permissible for a user to save work-related products of any type (e.g., documents, spreadsheets, etc.) to personal devices or personal removable media (e.g., flash drives, etc.).

E. Suspicious Activity Reporting

1. Users are required to report suspicious activities or incidents to the IT Help Desk, which will then report to the Information Security group.
2. Suspicious and potential phishing emails should be reported with tools provided in the email system and Department ticketing systems.

9. Remote Access, Authentication, and Devices

A. Remote Access

1. Connecting to internal State network resources must be done through approved remote access processes, using VPN for State computing resources accessible only on the trusted State private network; direct access is prohibited.
2. Users may not remotely access a CDOS or State IT resource via a personal device unless approved by the appointing authority.

B. International Access to State Data and IT Resources

1. International user access to systems and data from high-risk countries as defined by the State Department's International Traffic in Arms Regulations (ITAR) list is prohibited.
2. International user access to systems and data may be prohibited by laws governing specific data types, including but not limited to CJIS and FTI.
3. Users should reference CDOS HR policies and abide by State Policies for working out of State of Colorado and/or the country.

4. Accessing State or CDOS resources from other countries for any period of time must be approved by Human Resources and Information Technology.

10. Personal Use of State IT Resources

- A. Only minimal, incidental personal use of State resources such as email is allowed and never for political, business or any purpose that conflicts with State ethics requirements or State policies, and/or the Department's conflict of interest policy. (Reference Governor's Office of Information Technology Acceptable Use Policy (AUP) Adopted 12/19/2024 - <https://oit.colorado.gov/standards-policies-guides/technical-standards-policies>)

11. Use of Personally Owned Equipment

- A. When a user has been approved to use their personal device as their primary work device, they are responsible for ensuring that any device used to connect to a State IT resource is secured consistent with best practices for the use of personal computing devices, including without limitation:
 1. Ensure the device is free from malware infections.
 2. The device is protected by strong authentication.
 3. The device operating system and software are updated and current according to State standards.
 4. The device is utilizing full disk encryption.
 5. The device is not storing State data.
- B. Users are prohibited from using personally owned devices to access, store, or process State data without written authorization from both their Division Director or Deputy and the Director of Information Technology, Deputy Director of Information Technology, or the Appointing Authority.
- C. CDOS staff are permitted to use personal mobile devices for MFA authentication applications such as RSA Authentication, Google Authenticator, Last Pass Authenticator, and other authenticators listed on the Approved software list.
- D. It is not permissible to save work-related products of any type (e.g., documents, spreadsheets, etc.) to user personal devices or personal removable media (e.g., flash drives, etc.).

12. Training

- A. Cybersecurity Training
 1. All users are required to complete mandatory cybersecurity training at least annually and throughout the year as assigned.
 2. Users may be assigned additional cybersecurity or other training as necessary to ensure proper system use and security.
- B. Software and Systems Training
 1. Users in different divisions (Business, Elections, Administration, Information Technology) have distinct roles and responsibilities. Managers, in coordination with users, must determine training needs to ensure the proper handling of data and the proper use of Information Technology.

2. Users are required, according to their job function, to research and learn about the technologies needed to effectively complete their work. Users should work with their supervisor to determine their training needs.

13. Compliance

A. Privacy

1. Information transmitted through unsecured systems should not be considered private.
2. All transmissions are business records and subject to inspection, review, or disclosure as required by law.
3. The Department reserves the right to access and disclose all information sent, received, or stored through its systems.

B. License Agreements/Copyright Compliance

1. State IT resources must be used in accordance with the terms of software license agreements or other copyright restrictions to protect the state, its officials, and Users from possible legal action. Users may not access or store any copyrighted material using any State IT resource without an appropriate license.
2. The Department may be financially liable for unauthorized use of copyright-protected or licensed material and may seek restitution from employees responsible for unauthorized use of copyright-protected or licensed material.

C. Criminal Activity

1. Information created, collected, generated, or stored by a user on either State-owned computing devices or personal computing devices that are authorized to connect to State IT resources may be disclosed to State risk management, State human resources, Department human resources and State law enforcement if criminal activity is suspected. This disclosure will be at the discretion of CDOS Information Technology Senior Management, the User's appointing authority and State human resources, as applicable, during or after the course of investigating suspected acceptable use violations.

D. Employment Termination

1. As soon as possible prior to, and in all events at the latest upon the date of, termination of employment, Information Technology must be notified immediately to remove access to a user's various systems and facilities.

14. Monitoring and Enforcement

A. Information Systems and Security Operations

1. Information Technology management and the cybersecurity team will collaborate to monitor systems, collect logs, and conduct security assessments to verify compliance with established safeguards and behaviors outlined in this policy. Security personnel and system administrators will perform regular audits of system access, review application logs, monitor network traffic, conduct

penetration testing, and execute other security-related functions as authorized by CDOS Information Technology Senior Management or the State Chief Information Security Officer.

2. Systems administrators will back up, delete, retain, and restore data in alignment with the Department data retention policies.

B. Surveillance Authority

1. CDOS IT management, supervisors, and security personnel maintain the right to monitor all computing activities without prior notification. This monitoring encompasses all system access, including but not limited to Internet usage, file access, and email communications.
2. Any public agency has the right to monitor and/or investigate their users' activity while accessing State network, internet, system or email accounts and their usage, whether on a State-issued or personal device authorized to connect to the State network. (CISP-018)

C. Privacy and Colorado Open Records Act (CORA)

1. Users have no expectation of privacy while using State resources or technology. All electronic communications sent to and from State-assigned accounts are the property of the State of Colorado.
2. Electronic communications pertaining to State business are subject to the Colorado Open Records Act (CORA, C.R.S. § 24-72-201 et seq.). Any communication using personal equipment, such as personal phones or laptops, is also subject to CORA to the extent it pertains to State business.

15. Annual Acceptance, Retention, and Expiration

- A. This policy must be accepted by Users at the start of employment and no less frequently than annually thereafter.
- B. The following must be done by Agency and Users:
 1. CDOS provides a documented acknowledgment of these rules for Users to read and sign before accessing the system.
 2. CDOS maintains a record of signed acknowledgments for appropriate retention periods.
 3. CDOS requires individuals to re-read and re-sign the rules annually, regardless of prior acknowledgments.
- C. This policy remains in effect until superseded or rescinded by the CDOS Chief Information Security Officer or CDOS Chief Information Officer.

16. Definitions

- A. Access: The time when an individual is permitted into a security point or system. Access also means the authority to access restricted facts, information, or records.
- B. Appointing Authority: As defined in Board Rule 1-8, refers to the executive director of principal departments or their delegate(s).
- C. CDOS Information Technology Senior Management – Chief Information Officer, Deputy Chief Information Officer, Chief Information Security Officer, and Chief Technology Officer.
- D. CJIS Data: Refers to Criminal Justice Information Services, including fingerprints, criminal background checks, etc. CJIS includes Criminal history record information from the FBI; however, PII obtained through public records/court documents typically is no longer protected (once published).

- E. **Credentials and secrets:** In computer networks, secrets are sensitive digital credentials that provide access to systems, services, and data. Think of them as special keys that allow different parts of our technology systems to communicate securely with each other. Unlike regular passwords that humans use, secrets are designed to be used by machines, applications, and automated processes. Examples include:
 - 1. API keys that allow applications to communicate with each other,
 - 2. digital certificates for secure website connections,
 - 3. database passwords for accessing stored information,
 - 4. SSH keys for secure remote system access,
 - 5. encryption keys that scramble sensitive data,
 - 6. security tokens for temporary system access,
 - 7. private certificates for secure data transmission,
 - 8. cloud service credentials.
- F. **Data Owner:** CDOS Division Directors are ultimately responsible for the data that their Division is responsible for or maintains. Directors may designate staff as owners of specific datasets. Data owners and their designees are responsible for maintaining, reviewing, and ensuring proper data handling as outlined in this policy.
- G. **Disclosure of Information:** Making facts or information known to an individual, group or the public.
- H. **Encryption at rest:** Hard disk or local storage encryption, in other words, data that is stored or “at rest” and not “in transit”.
- I. **IT Resource:** Any computing device or resource, including but not limited to desktop computers, laptops, tablets (e.g., iPad, Windows, Chromebook, etc.); smartphones (e.g., iPhone, Android, etc.), removable media that has the ability to access IT resources, including IT networks; and accounts that allow access to IT resources (e.g., email, cloud-based software and applications, etc.).
- J. **Multi-factor authentication:** Consists of something you know like a password, something you have like a security token or authentication device, or something you are, such as your fingerprint. Two-factor MFA is reached when you use two of the three above to authenticate with a system.
- K. **PII:** Any information that can be used by itself or combined with other personal or identifying information to uniquely identify, contact or locate a specific person.
- L. **Remote Access:** Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network. (e.g., the Internet)
- M. **Removable Media:** Any type of storage device that can be removed from an IT resource to which it has been connected or attached, including but not limited to any USB drive (also called flash drive or thumb drive), hard drive, personal music player, disc drive, DVD, CD, camera, mobile phone, memory card, etc.
- N. **Sensitive Data or Information:** Information whose loss, misuse, or unauthorized access to or modification of which could adversely affect the interests or the ability of the Department or State to conduct day-to-day operations or the privacy of individual persons. Sensitive data or information includes, but is not limited to FTI, PII, PHI, CJI, etc. See TS-CISO-001 Data Security (posted on OIT’s website at Technical Standards & Policies).
- O. **Unauthorized Access:** A person gains logical or physical access without permission to a network, system, application, data, information, records, or other resource.

17. Revision History

<i>Review Date</i>	<i>Reviewed By</i>	<i>Revisions</i>
01/20/2025	Rich Schliep	Initial Draft

18. Acknowledgment

All users of CDOS networks as defined in the scope (Section 2) must sign this Acceptable Use Policy (AUP), agreeing to adhere to all policies and guidelines contained therein.

Any violation of the behaviors and safeguards established in this document constitutes unacceptable use and shall result in disciplinary measures. Such measures may include:

- Mandatory security awareness training
- Immediate access revocation
- Financial liability for damages
- Employment suspension or termination
- Civil or criminal prosecution under applicable laws

A violation of this policy by temporary workers, interns, volunteers, contractors, or vendors may result in termination of their contract or assignment with the State of Colorado or Colorado Department of State.

The Department reserves the right to implement any combination of these measures based on the severity and nature of the violation.

I acknowledge that I have read and understand the Acceptable Use Policy for State Data and IT Resources.

I agree to strictly abide by these policies and procedures and acknowledge that when an instance of non-compliance is suspected or discovered, proper disciplinary action may be taken, up to and including termination in accordance with Colorado regulations. Criminal or civil action may be initiated where appropriate.

Jena Griswold

Employee Name (printed)

Signed by:

Jena Griswold

1971F3C99C634D5...

Employee Signature

Administration

Division (printed)

May 2, 2025

Date

DocuSigned by:

Rich Schliep

C84D905A5DB9448...

Chief Information Officer Signature

May 6, 2025

Date